

1 ARAVIND SWAMINATHAN (*admitted pro hac vice*)
aswaminathan@orrick.com

2 REBECCA HARLOW (STATE BAR NO. 281931)
rharlow@orrick.com

3 THOMAS FU (STATE BAR NO. 325209)
tfu@orrick.com

4 ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
5 405 Howard Street
San Francisco, CA 94105-2669
6 Telephone: +1 415 773 5700
Facsimile: +1 415 773 5759

7 Attorneys for Defendant
8 Lead Intelligence, Inc. d/b/a Jornaya

9
10 UNITED STATES DISTRICT COURT
11 NORTHERN DISTRICT OF CALIFORNIA
12

13 LORETTA WILLIAMS, individually and on
behalf of all others similarly situated,

14 Plaintiff,

15 v.

16 DDR MEDIA, LLC, a Pennsylvania limited
17 liability company, d/b/a ROYAL MARKETING
GROUP, and LEAD INTELLIGENCE, INC., a
18 Delaware corporation, d/b/a Jornaya,

19 Defendants.
20
21
22
23
24
25
26
27
28

Case No. 3:22-cv-03789-SI

**DEFENDANT JORNAYA'S MOTION TO
DISMISS FOR FAILURE TO STATE A
CLAIM**

Date: June 2, 2023

Time: 10:00 a.m.

Judge: Hon. Susan Illston

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on June 2, 2023, at 10:00 a.m., or as soon thereafter as available, in the courtroom of the Honorable Illston, located at 450 Golden Gate Avenue, Courtroom 1, 17th Floor, San Francisco, California 94102 (via Zoom webinar), Defendant Lead Intelligence, Inc., d/b/a/ Jornaya (“Jornaya”), will and hereby does move to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6). This Motion is based on this Notice of Motion and Motion, the Memorandum of Points and Authorities, the pleadings and papers on file in this action, any other such matters of which the Court may take judicial notice, and any other matter that the Court may properly consider.

TABLE OF CONTENTS

	Page
I. STATEMENT OF ISSUES TO BE DECIDED	2
II. SUMMARY OF RELEVANT FACTS	2
III. LEGAL STANDARD.....	3
IV. LEGAL ARGUMENT.....	3
A. The FAC Fails To State A Claim Under Section 631.....	3
1. The FAC fails to state a claim under either clause of Section 631(a), because it fails to plead facts showing that Jornaya was a third party to Plaintiff’s communications.....	4
2. The FAC fails to state a claim under either clause of Section 631(a), because it fails to plead facts showing that Jornaya intercepted a communication “in transit.”..	6
B. The FAC Fails to State a Claim Under the UCL.	9
C. The FAC Fails to State a Claim for Invasion of Privacy Because It Does Not Allege Facts Showing That Jornaya Committed an “Egregious” Privacy Violation.	9
V. CONCLUSION.....	10

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	3
<i>Birdsong v. Apple, Inc.</i> , 590 F.3d 955 (9th Cir. 2009)	9
<i>Byars v. Hot Topic, Inc.</i> , 2023 WL 2026994 (C.D. Cal. 2023).....	4, 5
<i>Cline v. Reetz-Laiolo</i> , 329 F. Supp. 3d 1000 (N.D. Cal. 2018)	6
<i>Cody v. Boscov's, Inc.</i> , 2023 WL 2338302 (C.D. Cal. 2023).....	4
<i>Ehret v. Uber Tech., Inc.</i> , 68 F. Supp. 3d 1121 (N.D. Cal. 2014)	9
<i>In re Facebook Privacy Litig.</i> , 791 F. Supp. 2d 705 (N.D. Cal. 2011)	9
<i>In re Facebook, Inc. Internet Tracking Litig.</i> , 956 F.3d 589 (9th Cir. 2020)	4
<i>Folgelstrom v. Lamps Plus, Inc.</i> , 195 Cal. App. 4th 986 (2011)	10
<i>Gonzalez v. Planned Parenthood of L.A.</i> , 759 F.3d 1112 (9th Cir. 2014)	3
<i>In re Google Assistant Privacy Litig.</i> , 457 F. Supp. 3d 797 (N.D. Cal. 2020)	7, 9, 10
<i>In re Google, Inc. Privacy Policy Litig.</i> , 58 F. Supp. 3d 968 (N.D. Cal. 2014)	10
<i>Graham v. Noom, Inc.</i> , 533 F. Supp. 3d 823 (N.D. Cal. 2021)	4
<i>Johnson v. Blue Nile, Inc.</i> , 2021 WL 1312771 (N.D. Cal. 2021)	4
<i>Konop v. Hawaiian Airlines, Inc.</i> , 302 F.3d 868 (9th Cir. 2002)	6

1	<i>Licea v. Am. Eagle Outfitters, Inc.</i> ,	
2	2023 WL 2469630 (C.D. Cal. 2023).....	7
3	<i>Licea v. Cinmar, LLC</i> ,	
4	2023 WL 2415592 (C.D. Cal. 2023).....	4, 5, 6
5	<i>Low v. LinkedIn Corp.</i> ,	
6	900 F. Supp. 2d 1010 (N.D. Cal. 2012)	9
7	<i>Mastel v. Miniclip SA</i> ,	
8	549 F. Supp. 3d 1129 (E.D. Cal. 2021).....	9
9	<i>Sprewell v. Golden State Warriors</i> ,	
10	266 F.3d 979 (9th Cir. 2001)	7
11	<i>Underhill v. Kornblum</i> ,	
12	2017 WL 2869734 (S.D. Cal. 2017)	6, 7
13	<i>Verizon v. FCC</i> ,	
14	740 F.3d 623 (D.C. Cir. 2014).....	7
15	<i>In re Vizio, Inc. Consumer Privacy Litig.</i> ,	
16	238 F. Supp. 3d 1204 (C.D. Cal. 2017)	6, 7
17	<i>Warden v. Kahn</i> ,	
18	99 Cal. App. 3d 805 (1979)	4
19	<i>Williams v. What If Holdings, LLC</i> ,	
20	2022 WL 17869275 (N.D. Cal. 2022)	4, 5
21	<i>Yale v. Clicktale, Inc.</i> ,	
22	2021 WL 1428400 (N.D. Cal. 2021)	4
23	Statutes	
24	Cal. Penal Code § 631(a)	<i>passim</i>
25	California Unfair Competition Law	1, 9
26	Telephone Consumer Protection Act	1, 2, 3, 5
27	Rules	
28	Federal Rule of Civil Procedure 12(b)(6)	2, 3
	Other Authorities	
	California Constitution.....	3, 9, 10

1 This action seeks to outlaw—indeed, to criminalize—important technology tools used by
 2 online comparison shopping and “lead-generation” companies to comply with federal law and
 3 document their compliance. For example, consumers looking for a loan (e.g., a home mortgage)
 4 often turn to websites (known as both comparison shopping sites or “lead sellers”) that help source
 5 quotes from multiple lenders. Those websites collect basic information from the consumer—e.g.,
 6 income bracket, loan size, ZIP code—and then share it (with permission) with various lenders who
 7 then get in touch with the consumer, often through text messaging and calling services, which must
 8 comply with the Telephone Consumer Protection Act (TCPA). That process only works, though,
 9 if the lenders can trust that the information they receive from the lead seller—particularly the
 10 consumer consent—is legitimate. For instance, a lead seller may *tell* a lender that the consumer
 11 gave consent to receive phone calls about a quote for a potential mortgage. But if that proves to be
 12 inaccurate or if the lender cannot produce proof of the valid information and consent, the liabilities
 13 under the TCPA can be enormous.

14 Lead Intelligence Inc. d/b/a Jornaya (“Jornaya”) is an innovative technology company that
 15 helps firms prove the origin and compliance of the data they are buying or selling. Specifically,
 16 both lead sellers and lead buyers use Jornaya’s product TCPA Guardian to validate whether
 17 visitors interacting with their site in fact provided the prior express consent required by the TCPA,
 18 and to produce evidence of that consent for use in compliance programs (and, if necessary, in
 19 litigation), by capturing certain information website visitors enter into the website.

20 In this lawsuit, Plaintiff claims that TCPA Guardian itself is unlawful, and allege that
 21 Jornaya and another defendant, DDR Media, LLC (“DDR Media”), committed a crime by
 22 (respectively) making that software available for purchase and installing it on DDR Media’s
 23 website to capture “keystrokes and clicks,” that reflected her “name, address, and phone number,”
 24 as well as “the date and time of the visit, her IP address, and her geographic location,” in purported
 25 violation of the California’s Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 631; the
 26 California Constitution; and the Unfair Competition Law (“UCL”).¹ On that basis, Plaintiff seeks

27 ¹ Notwithstanding various inaccuracies in the First Amended Complaint (“FAC”), this Motion to
 28 Dismiss accepts the FAC factual allegations as true for the sole purpose of showing that Plaintiff
 still nevertheless fails to state a claim under Rule 12(b)(6).

1 not only an injunction that would prohibit TCPA Guardian’s use, but also \$5,000 in statutory
2 damages for each supposed class member.

3 Unsurprisingly, Plaintiff’s gambit fails for multiple reasons. Her **Section 631** claim fails
4 (among other reasons), because: (1) Section 631 prohibits only eavesdropping by an undisclosed
5 *third party*, whereas the First Amended Complaint (“FAC”) here alleges nothing more than a
6 website provider using a software tool *on its own* website; (2) Section 631 applies only to
7 communications intercepted *in transit*, whereas here the FAC alleges that TCPA Guardian runs on
8 DDR Media’s website, and so could act only *after* Plaintiff’s information reached its intended
9 destination; and (3) Section 631 applies only to the interception of a message’s substantive
10 *contents*, but all of the information alleged to have been collected here (e.g., name, address) has
11 been specifically held by courts *not* to be contents. Her **Unfair Competition Law** claim fails
12 because that law requires that the plaintiff suffered a loss of money or property—which Plaintiff
13 does not (and cannot) allege here. And her **invasion of privacy** claim fails because that cause of
14 action requires an “egregious breach of the social norms” beyond even wrongful disclosure of a
15 Social Security Number, whereas Plaintiff’s claims here are based solely on far less sensitive
16 information. Accordingly, Plaintiff’s FAC must be dismissed with prejudice.

17 **I. STATEMENT OF ISSUES TO BE DECIDED**

18 Jornaya seeks an order pursuant to Federal Rule of Civil 12(b)(6) dismissing the suit for
19 failure to state a claim.

20 **II. SUMMARY OF RELEVANT FACTS**

21 Jornaya is a consumer journey insight platform that provides marketers, data analysts, and
22 compliance professionals with the highest-resolution view of the consumer buying journey. One
23 of the tools developed by Jornaya is a product known as TCPA Guardian, a compliance tool that
24 helps companies comply with the Telephone Consumer Protection Act (TCPA), a federal law that
25 requires prior written consent before making an autodialed call to a cell phone number. Jornaya
26 licenses TCPA Guardian to companies so they have the ability to validate whether each visitor
27 interacting with their website provided the prior express consent required by the TCPA, including
28 access to a visual rendering of the visitor entering their consent (e.g., by requesting that the

1 company call them, and checking a box indicating consent to be contacted) on the website. This
 2 allows companies to assure themselves that the consumer can safely be contacted without running
 3 afoul of the TCPA, and to provide evidence of TCPA compliance in the event a TCPA complaint
 4 is filed. In so doing, TCPA Guardian helps both companies and consumers be assured that the
 5 TCPA's strictures are complied with.

6 In June 2022, Plaintiff sued Jornaya as well as DDR Media, who implemented Jornaya's
 7 technology on its website snappyrent2own.com. Although the FAC is light on facts, the basic gist
 8 of the allegations is that Jornaya's technology unlawfully recorded certain of Plaintiff's
 9 interactions with snappyrent2own.com—namely, her entering her name, address, and phone
 10 number into snappyrent2own.com, as well as IP address and geographic location. FAC ¶¶ 21-22.
 11 On this basis, Plaintiff asserts that Jornaya violated the California Invasion of Privacy Act (CIPA),
 12 Cal. Penal Code § 631; the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200;
 13 and the California Constitution.

14 **III. LEGAL STANDARD**

15 To survive a motion to dismiss under Rule 12(b)(6), “a complaint must contain sufficient
 16 factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v.*
 17 *Iqbal*, 556 U.S. 662, 678 (2009). “Threadbare recitals of the elements of a cause of action,
 18 supported by mere conclusory statements, do not suffice.” *Id.* (citation omitted). While a court
 19 must accept all material factual allegations as true, it is not required to accept as true any
 20 allegations that are contradicted by matters that are subject to judicial notice, that are exhibits to a
 21 complaint, or that are incorporated by reference in a complaint. *See, e.g., Gonzalez v. Planned*
 22 *Parenthood of L.A.*, 759 F.3d 1112, 1115 (9th Cir. 2014).

23 **IV. LEGAL ARGUMENT**

24 **A. The FAC Fails To State A Claim Under Section 631.**

25 Under Section 631, it is unlawful to (1) “intentionally tap[] ... any telegraph or telephone
 26 wire, line, cable, or instrument,” or (2) “willfully and without the consent of all parties to the
 27 communication ... reads, or attempts to read, or to learn the contents or meaning of any message,
 28 report, or communication while the same is in transit.” Cal. Penal Code § 631(a). It is also

1 unlawful to “aid[], agree[] with, employ[], or conspire[] with any person” to do either of those
 2 things. *Id.* Plaintiff has failed to allege a violation of Section 631 for several reasons.

- 3 1. *The FAC fails to state a claim under either clause of Section 631(a), because*
 4 *it fails to plead facts showing that Jornaya was a third party to Plaintiff’s*
communications.

5 The FAC fails to state a claim against Jornaya under any clause of Section 631 because it
 6 fails to allege facts showing that Jornaya was a third party to Plaintiff’s communications. Section
 7 631 “‘appl[ies] only to eavesdropping by a third party.’” *In re Facebook, Inc. Internet Tracking*
 8 *Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (quoting *Warden v. Kahn*, 99 Cal. App. 3d 805, 811
 9 (1979); *see also, e.g., Cody v. Boscov’s, Inc.*, 2023 WL 2338302, at *2 (C.D. Cal. 2023)
 10 (collecting cases); *see also, e.g., Byars v. Hot Topic, Inc.*, 2023 WL 2026994, *8-*9 (C.D. Cal.
 11 2023). It does not cover “a participant”—even one who “record[s]” the communication. *In re*
 12 *Facebook*, 956 F.3d at 607; *see also, e.g., Licea v. Cinmar, LLC*, 2023 WL 2415592, at *7 (C.D.
 13 Cal. 2023).

14 Here, that rule means that DDR Media cannot be liable under Section 631(a), as DDR
 15 Media was the intended recipient of Plaintiff’s information. *See* FAC ¶¶ 20-21. It also means that
 16 Jornaya cannot be liable either. That is because Jornaya would be considered to be an
 17 impermissible “third party” to Plaintiff’s communications ***only if*** “Plaintiff ... provide[s] facts
 18 suggesting that [Jornaya is] recording [DDR Media]’s customers’ information for some use or
 19 potential future use beyond simply supplying this information back to [DDR Media].” *Cody*, 2023
 20 WL 2338302, at *2; *accord, e.g., Byars*, 2023 WL 2026994, at *9. Absent such allegations,
 21 Jornaya stands accused of doing nothing more than supply “software [that] was merely a tool that
 22 [DDR Media] used to record its own communications with plaintiff”—which courts have
 23 repeatedly held is not a crime under Section 631. *See Williams v. What If Holdings, LLC*, 2022
 24 WL 17869275, at *3 (N.D. Cal. 2022) (citing *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 832–33
 25 (N.D. Cal. 2021); *Johnson v. Blue Nile, Inc.*, 2021 WL 1312771, at *3 (N.D. Cal. 2021); *Yale v.*
 26 *Clicktale, Inc.*, 2021 WL 1428400, at *3 (N.D. Cal. 2021); *In re Facebook Inc. Internet Tracking*
 27 *Litig.*, 956 F.3d at 608).

Plaintiff’s FAC, however, is entirely devoid of allegations that Jornaya “aggregates,” “otherwise processes,” or “independently uses” the recorded data. *Byars*, 2023 WL 2026994, at *9 (quoting *Williams*, 2022 WL 17869275, at*3). To the contrary, the FAC alleges that Jornaya’s TCPA Guardian product collects and stores data at DDR Media’s direction, *see* FAC ¶ 11, and for DDR Media’s benefit—namely, to facilitate DDR Media’s “compliance with the federal Telephone Consumer Protection Act” and to provide DDR Media with “evidence of prior express consent to receive telemarketing calls” in the event of a TCPA complaint. FAC ¶ 5; *see also id.* ¶ 10 (alleging that this is a “primary reason why DDR Media contracts with Jornaya for the TCPA Guardian product”). Those allegations are indistinguishable from ones that courts have held to be “not enough” to survive a motion to dismiss. *Williams*, 2022 WL 17869275 at *3 (allegations that websites “deployed [the vendor’s] recording software only on [the] websites and that the recordings were stored and accessed on [the vendor’s] servers” were insufficient to show that the vendor was a third party under Section 631). As one court recently put it: “When a party captures and stores data, courts have found that they operate like an extension of the defendant (i.e. a tape recorder),” and hence cannot be liable under Section 631. *Cinmar*, 2023 WL 2415592, at *8. That is exactly what Plaintiff alleges here. And so for this reason, her Section 631 claim fails.

Said simply, Plaintiff’s FAC establishes nothing more than that Jornaya is “a vendor that provides a software service” to DDR Media—namely, tools that “capture its clients’ data, hosts it on [Jornaya]’s servers, and allows the clients to analyze their data.” *Byars*, 2023 WL 2026994, at *10; *see also* FAC ¶ 25. Far from being a “third party” making its own decision to interlope on Plaintiff’s communications with DDR Media, Jornaya simply “provide[d] a tool” that DDR Media chose to employ “to record and analyze its own data in aid of [its own] business.” *Byars*, 2023 WL 2026994, at *10. Jornaya thus has no independent involvement in this case; it acts only “an extension of [DDR Media].” *Id.* Thus, because DDR Media is a party (outside the scope of Section 631), so too is Jornaya.

Because Jornaya was not a third party to any of Plaintiff’s communications, it cannot be deemed to have violated Section 631(a).

2. The FAC fails to state a claim under either clause of Section 631(a), because it fails to plead facts showing that Jornaya intercepted a communication “in transit.”

The Section 631(a) claim also fails because the FAC fails to plead facts showing that Jornaya intercepted a communication in transit pursuant to the statute. Section 631(a) liability attaches only when a defendant has committed “the *interception* of an electronic communication.” *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1050-51 (N.D. Cal. 2018). Per the statute’s text, this means that the defendant must wrongfully access a communication while it is “in transit.” Cal. Penal Code § 631(a). Courts interpret Section 631(a)’s “in transit” requirement consistent with its federal analogue, the Wiretap Act—*i.e.*, narrowly and to require “acquisition contemporaneous with transmission.” *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (holding that the “narrow” definition of “intercept” applies to electronic communications to mean “acquisition of contemporaneous with transmission-with respect to wire communications”).

To survive a motion to dismiss, a Section 631(a) claim must thus allege facts that show that the alleged reading or acquiring of the communication’s content occurred while the communication was *en route* to its destination—not after it had already arrived. *See Underhill v. Kornblum*, 2017 WL 2869734, at *5 (S.D. Cal. 2017) (dismissing claim because plaintiff had not pled facts demonstrating that defendant acquired the communications contemporaneously with their transmission). Conclusory assertions that merely recite that the communications were acquired “during transmission” or “in real time” are insufficient. *See In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017) (dismissing Section 631(a) claim because allegations that defendant “intercepted their communications ... ‘during transmission’” were too conclusory). Rather, a complaint must “articulate[] with sufficient clarity when [defendant] supposedly intercepted their communications.” *See id.*

Plaintiff’s FAC provides no well-pled factual allegations that would show that Jornaya accessed Plaintiff’s information while it was traveling to DDR Media, as opposed to *after* it had reached its destination. The FAC’s bare assertions that Plaintiffs’ “communications [were] intercepted” or captured “real time,” FAC ¶¶ 2, 6, 28, are identical to those that courts have already found lacking. *See Cinmar*, 2023 WL 2415592, at *10 (“Plaintiffs must provide more than

conclusory allegations that messages were ‘intercepted in real time.’”); *Licea v. Am. Eagle Outfitters, Inc.*, 2023 WL 2469630, at *9 (C.D. Cal. 2023) (same); *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d at 1228; *Underhill*, 2017 WL 2869734, at *4. And to the extent the FAC does provide factual allegations about how or when the purported interception occurred, they tend to suggest that it was only *after* the information arrived at its intended destination (DDR Media’s website), as they allege that the Jornaya code that supposedly performed the recording was “installed” by DDR Media and “embed[ed]” in DDR Media’s website. FAC ¶ 11. The FAC thus fails to state a claim under either clause of Section 631(a), because it fails to allege facts showing that interception occurred “in transit.”

a. The FAC fails to allege a violation of Section 631(a)’s first clause, because it fails to allege a wiretap of a telephone line.

In any event, the FAC separately fails to state a claim under the first clause of Section 631(a), which makes a defendant liable only if it taps a “telegraph or telephone wire, line, cable, or instrument.” Cal. Penal Code § 631(a). That clause requires a plaintiff to allege not only that a defendant tapped a “wire, line, cable, or instrument” but, also that whichever of those was involved carried “telegraph or telephone” signals. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 825-26 (N.D. Cal. 2020) (holding that complaint failed to state a claim under Section 631(a) because it did not suggest “that Google Assistant operates using telegraph or telephone wires”). Here, the FAC alleges no facts suggesting that any services Jornaya provides to DDR Media operate via (much less “tap”) “telegraph or telephone” lines. In fact, it says otherwise, alleging that Jornaya’s technology “tapped the lines of communication between Plaintiff ... and DDR Media’s websites”—a “communication” that occurred not over the phone but over the “internet.” FAC ¶¶ 41, 45; *see also Sprewell v. Golden State Warriors*, 266 F.3d 979, 988-89 (9th Cir. 2001) (affirming dismissal because plaintiff’s complaint included “unnecessary details contrary to his claims”). There is no serious dispute that “internet communication” no longer occurs over “telephone” or “telegraph” lines, *see Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014), so the allegation about internet communications therefore negates the requisite “telegraph or telephone” lines element, and hence any claim under Section 631(a)’s first clause.

b. The FAC fails to allege a violation of Section 631(a)'s second clause because it fails to plead facts showing that Jornaya read the "contents" of any message.

The FAC separately fails to state a claim under Section 631(a)'s second clause, because it fails to allege that Jornaya unauthorizedly access "the 'contents' of any communication." *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020). As with the federal Wiretap Act, Section 631 does not make it a crime to access any information passed between two parties, but rather only the substantive "contents" of a communication—i.e., "the intended message conveyed by the communication." *See In re Zynga Privacy Litig.*, 750 F. 3d 1098, 1106 (9th Cir. 2014). That means to show a violation of Section 631, two things must be true: (1) a plaintiff must have intended to convey a substantive message, and (2) an unauthorized party must have accessed (or attempted to access) that substance, and not mere "record information," like a person's name or address. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (holding that "data" that is "generated" without the communicative "intent of the user" cannot "constitute 'content' susceptible to interception").

Plaintiff claims that Jornaya's technology captured her "keystrokes and clicks on the website," which conveyed her "name, address, and telephone number," "the date and time of the visit, her IP address, ... her geographic location." FAC ¶¶ 21-23. But all of those types of data—i.e., name, address, telephone number, visit date, IP address, and geographic location—have been squarely held not to constitute message "contents" under Section 631(a). *See Svenson v. Google Inc.*, 65 F. Supp. 3d 717, 729 (N.D. Cal. 2014) (explaining that "names, mailing addresses, phone numbers," are not "contents" of a communication); *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (recording the "date" of communications "does not capture the contents of communications"); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1084–85 (N.D. Cal. 2018) ("IP address" is "not the contents of a communication within the meaning of the Act"); *Brodsky v. Apple Inc.*, 2019 WL 4141936, at *6 (N.D. Cal. 2019) ("geographic location information [is] not contents"). Accordingly, Plaintiff's Section 631 claim fails for this independent reason.

B. The FAC Fails to State a Claim Under the UCL.

To state a claim under the UCL, a plaintiff must (among other requirements) demonstrate UCL standing, which is distinct from—and requires a higher showing than—Article III standing. *Ehret v. Uber Tech., Inc.*, 68 F. Supp. 3d 1121, 1132 (N.D. Cal. 2014). Specifically, “[w]hereas a federal plaintiff’s injury in fact [for purposes of Article III standing] may be intangible and need not involve lost money or property, ... a UCL plaintiff’s ‘injury in fact’ [must] specifically involve lost money or property.” *Id.* Said otherwise, to establish standing under the UCL, a plaintiff “must establish that [she] (1) suffered an injury in fact and (2) lost money or property as a result of the unfair competition.” *Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009).

But Plaintiff has not alleged any economic injury as a result of Jornaya’s or DDR Media’s conduct. Instead, the supposed harm underlying her FAC is that she was “unlawfully monitored” while using DDR Media’s website. But “[n]umerous courts have held that disclosure of personal information alone does not constitute economic or property loss sufficient to establish UCL standing.” *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1144 (E.D. Cal. 2021); *see also, e.g., In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (“A plaintiff’s ‘personal information does not constitute property under the UCL.”), *aff’d* 572 F. App’x 494 (9th Cir. 2014). Accordingly, Plaintiff cannot state a claim under the UCL.

C. The FAC Fails to State a Claim for Invasion of Privacy Because It Does Not Allege Facts Showing That Jornaya Committed an “Egregious” Privacy Violation.

Finally, the FAC fails to allege facts anywhere near sufficient to state a claim for invasion of privacy. To allege a violation of California’s constitutional right to privacy, the FAC must allege, among other things, “conduct by the defendant that amounts to a serious invasion of [a] protected privacy interest.” *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 829 (N.D. Cal. 2020). To show the requisite “serious invasion” of privacy, the FAC must allege facts showing an “egregious breach of the social norms”—a “high bar” that is not satisfied by “[e]ven disclosure of personal information, including social security numbers.” *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012). “[C]ollection—and even disclosure to certain third parties—of” more anodyne personal information falls well below the requisite threshold. *In re*

1 *Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 829-30; *see also In re Google, Inc. Privacy*
 2 *Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (no intrusion claim based on collection and
 3 disclosure of users' data, including browsing histories); *Low*, 900 F. Supp. 2d at 1025 (no "highly
 4 offensive" invasion of privacy by disclosing users' browsing histories to third parties). Where a
 5 party does nothing more than engage in "routine commercial behavior," it does not commit a
 6 violation of California's constitution or common-law privacy protections. *In re Google Assistant*
 7 *Priv. Litig.*, 457 F. Supp. 3d at 830. That is true even where the "routine commercial behavior"
 8 involves "obtaining [a] plaintiff's address without his knowledge or permission, and using it to
 9 mail him coupons and other advertisements." *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th
 10 986, 992 (2011) (finding such conduct not an "egregious breach of social norms").

11 Here, the FAC fails to establish that Jornaya's conduct was even as egregious as conduct
 12 held insufficient elsewhere. What the FAC accuses Jornaya of doing—collecting innocuous
 13 information that is freely shared (name, address, telephone number)—happens on countless
 14 websites. Indeed, many websites lawfully collect far more, and more invasive, information. *See*
 15 *In re Pharmatrak, Inc.*, 329 F.3d 9, 14 (1st Cir. 2003) ("Cookies often store user preferences, login
 16 and registration information, or information related to an online 'shopping cart.'"). Because the
 17 FAC has alleged no facts that mark Jornaya's conduct as being particularly egregious—and
 18 certainly no facts rising even to the level of wrongful disclosure of Social Security Numbers—her
 19 constitutional privacy claims fail.

20 **V. CONCLUSION**

21 For the foregoing reasons, this Court should dismiss her FAC on the merits with prejudice.
 22
 23
 24
 25
 26
 27
 28

1 DATED: April 13, 2023

Respectfully Submitted,

2 ORRICK, HERRINGTON & SUTCLIFFE LLP

3
4 By: /s/ Rebecca Harlow

5 REBECCA HARLOW

6 Attorneys for Defendant, LEAD
INTELLIGENCE, INC. D/B/A JORNAYA